UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Norfolk Division

UNITED STATES OF AMERICA

v. **CRIMINAL NO. 2:16cr92**

ROBERT MCLAMB,

Defendant.

MEMORANDUM OPINION AND ORDER

This matter comes before the court on the Defendant's First Motion to Suppress, Second Motion to Suppress, and Motion to Compel. ECF Nos. 14, 15, 16. In his Motions to Suppress, the Defendant seeks to suppress evidence the government obtained, pursuant to a warrant, through use of the Network Investigative Technique ("NIT") code that enabled the government to access information on the Defendant's personal computer. First Mot. to Suppress at 1; Second Mot. to Suppress at 1. In his Motion to Compel, the Defendant seeks to compel discovery of two components of the NIT: (1) the unique identifier generator, and (2) the exploit source code. Mot. to Compel at 1. After full briefing and a hearing on the Motions, the matter is ripe for decision. For the reasons stated herein, these Motions to Suppress and the Motion to Compel are **DENIED**.

I. FACTUAL BACKGROUND

The Defendant was charged following an investigation into a website called "Playpen," which the government asserts operated as a child pornography site. First Mot. to Suppress at 4. The Playpen website was unusual in that it operated on what is known as the "Tor" network. See id. The Tor network enables its users to conceal their Internet Protocol ("IP") addresses, after they download the Tor browser from the Tor website. See id. IP addresses, if not hidden by either manual configuration or use of the Tor browser, can readily identify users. See Resp. to First Mot. to Suppress at 6. The Tor network aims to provide both users and operators of websites on the Tor network with anonymity. See id. Tor network users can use Tor indexes to locate these hidden services, which cannot be located on typical search engines, such as Google. See First Mot. to Suppress at 16. User communications on the Tor network are transmitted to various points among a network of computers before reaching their ultimate destination computer, and this makes identifying information, like IP addresses, more difficult to discover. Resp. to First Mot. to Suppress at 5. The government, however, can still recover identifying information, despite Tor network use, by way of the NIT. Id. at 7.

On February 19, 2015, the Federal Bureau of Investigation ("FBI") arrested the then-operator of Playpen, gained control of

the Playpen website, and thereafter operated it on a server in Virginia. Macfarlane Aff., ECF No. 14-2, ¶ 30. On February 20, 2015, the government obtained a warrant ("NIT Warrant") enabling it to use the NIT to investigate Playpen users. NIT Search Warrant and Application, ECF 19-9. The Defendant and the government disagree on the NIT's operation, but the basic concept is that, after a computer user logged into Playpen with a username and password, an application was authorized to send code, or computer instructions, to the user's computer. This code instructed the computer to send identifying information to a different, government-controlled computer.[1]

While the NIT warrant authorized the NIT to be deployed as soon as a user logged into Playpen, here, the NIT was not deployed until a posting thread in the "kinky fetish—zoo subforum" was accessed. Resp. to Mot. to Compel at 18. After deploying the NIT, the FBI was able to identify an IP address associated with a particular Playpen username ("slutwhore") and trace that username to the Defendant. Resp. to First Mot. to

[1] This identifying information included: (1) the activating computer's IP address, and the date and time that the NIT determined what that IP address was; (2) a unique identifier generated by the NIT; (3) the type of operating system running on the computer, including type, version, and architecture;(4) information about whether the NIT has already been delivered to the activating computer; (5) the activating computer's Host Name; (6) the activating computer's active operating system username; and (7) the activating computer's media access control ("MAC") address. NIT Search Warrant and Application at 4.

Suppress at 7. On December 1, 2015, the government obtained a residential search warrant ("Second Warrant") for the Defendant's home. The Second Warrant was executed on December 8, 2015, while the Defendant was home. Id. at 8. The Defendant acknowledged to agents that he viewed child pornography and that "slutwhore" was his username. See id. Child pornography was found on electronic devices owned by the Defendant during the execution of the Second Warrant. Id.

The parties do not dispute that Playpen's content included child pornography; rather, the Defendant takes issue with the NIT Warrant Application's description of the Playpen homepage. First Mot. to Suppress at 2-3. Although the NIT Warrant Application describes the homepage as displaying an image of partially clothed, prepubescent girls with their legs spread apart, the photo displayed on the homepage at the time of the application was actually one of a young girl with her legs crossed, wearing thigh-high fishnet stockings and a short dress or top that exposed her uncovered upper thighs. First Mot. to Suppress at 8-9; Resp. to First Mot. to Suppress at 14-15, 31.

II. PROCEDURAL HISTORY

On June 22, 2016, a federal grand jury returned an indictment, which charged McLamb with four counts of receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2), and one count of possession of child pornography, in violation of

18 U.S.C. § 2252(a)(4). ECF No. 1. The court set a preliminary motions deadline of July 29, 2016. ECF No. 10. The parties' agreed discovery order was filed on July 1, 2016. ECF No. 11. On July 29, 2016, the defense wrote a letter to the government seeking discovery of further information.[2] ECF No. 21-5. The government responded by letter on that same day, indicating that it did not intend to provide the requested source code or discovery on the unique identifier generator. ECF No. 21-6.

The Defendant filed the First and Second Motions to Suppress and the Motion to Compel Discovery, on July 29, 2016. ECF Nos. 14, 15, 16. The First and Second Motions to Suppress requested evidentiary hearings. The government filed its Responses on August 12, 2016. ECF Nos. 19, 20, 21. The Defendant filed Replies to these Responses on August 17, 2016. ECF Nos. 27, 28, 29. On August 22, 2016, the Defendant filed a Notice of Request for a Hearing on his First Motion to Suppress, Second

[2] The discovery sought by the Defendant included "copies of the source code for all software that the government used to identify Mr. Mclamb, including the payload or 'NIT'; the exploit; the 'unique identifier' generator; and the server software." ECF No. 21-5 at 1. In the Motion to Compel Discovery, the Defendant asks the court to compel production of "the source code or programming code for the exploit that the government used to gain access to Mr. McLamb's computer" and "the unique identifier generator through which the government purports to link Mr. McLamb to particular activity on the Playpen website." Mot. to Compel at 1. The Defendant's expert, Dr. Matthew Miller, defines "exploit" as "a piece of software that takes advantage of a flaw in a computer system." Miller Decl., ECF No. 16-3 at 2.

Motion to Suppress, and Motion to Compel. ECF No. 30. The court held a hearing on the Motions to Suppress and Motion to Compel on November 1, 2016. ECF No. 39. At the hearing, FBI Special Agent McFarlane was called as a witness by telephone, as agreed upon by the parties. See Joint Motion to Continue Trial, ECF No. 36 at 2.

III. FIRST MOTION TO SUPPRESS

A. Legal Standard

When police undertake a search in order to discover evidence of a crime, the Fourth Amendment's reasonableness standard generally requires them to obtain a search warrant. Riley v. California, 134 S. Ct. 2473, 2482 (2014)(quoting Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 653 (1995)). A successful application for a search warrant must be sufficient to support a finding of probable cause by a neutral, detached magistrate. United States v. Leon, 468 U.S. 897, 915 (1984). Probable cause requires that, given the totality of the circumstances, "there is a fair probability that contraband or evidence of a crime will be found in a particular place." Illinois v. Gates, 462 U.S. 213, 238 (1983). If a defendant shows that the affiant included a false statement knowingly and intentionally, or with reckless disregard for the truth, in the warrant affidavit and that false statement is necessary to find probable cause, the defendant is entitled to a hearing on the

inaccuracies. Franks v. Delaware, 438 U.S. 154, 171 (1978). When reviewing a magistrate's determination of probable cause, district courts should award it "great deference," declining to defer only when the finding was not supported by substantial evidence in the record or when the basis of the determination was a knowingly or recklessly false affidavit. Leon, 468 U.S. at 914-15.

Even if a violation of the Fourth Amendment occurs, "suppression is not an automatic consequence." Herring v. United States, 555 U.S. 135, 137 (2009). Rather, suppression is only appropriate where the blameworthiness of the police and the potential to deter police misconduct justify exclusion. Id. The exclusionary rule is a remedy of last resort; it is not an individual right. Id. at 140-41. The positive impacts of exclusion must outweigh the negative impacts of exclusion in order to merit application of the rule. Id. at 141. In accordance with these principles, evidence seized under a warrant that is invalid for lack of probable cause should not be excluded, if the police acted in good faith, defined as objectively reasonable reliance on the issued warrant. Id. at 142. Importantly, "when police mistakes are the result of negligence . . . rather than systematic error or reckless disregard of constitutional requirements," exclusion is improper. Id. at 147-48.

B. Analysis

In the Defendant's First Motion to Suppress, he argues that the fruits of the search conducted pursuant to the NIT Warrant should be suppressed for three reasons: (1) the NIT Warrant was unsupported by probable cause; (2) the FBI misled the issuing court with its description of Playpen's homepage; and (3) the NIT Warrant was an anticipatory warrant for which the triggering event establishing probable cause did not occur. First Mot. to Suppress at 2-3. While the particulars of these three issues differ, all three share the same premise: probable cause to search the computers of Playpen users did not exist following the change to the images on Playpen's homepage. Accordingly, if the finding of probable cause did not require the original images displayed on the homepage, the Defendant's three arguments are meritless.

Courts in the Eastern District of Virginia have already ruled that this exact image change was not material to the probable cause determination. See, e.g., United States v. Matish, No. 4:16cr16, 2016 WL 3545776, at *2, *12 (E.D. Va. June 21, 2016)(Morgan, J.); United States v. Darby, No. 2:16cr36, 2016 WL 3189703, at *9 (E.D. Va. June 3, 2016)(Doumar, J.). Additionally, the courts in this district ruled that, even if the image change had been material, suppression would be improper. See, e.g., Matish at *2, *12; United States v. Eure,

No. 2:16cr43, 2016 WL 4059663, at *7 (E.D. Va. July 28, 2016) (Doumar, J.). The court finds no reason to depart from these rulings, as explained below.

1. Neither the Issuance nor the Execution of the NIT Warrant Violated the Fourth Amendment

In his First Motion to Suppress, the Defendant argues that the search of his home computer was undertaken pursuant to a warrant unsupported by probable cause. Because the Magistrate's probable cause determination is awarded great deference, the Defendant would need to show that the finding was not supported by substantial evidence in the record, or that the finding was based on a knowingly or recklessly false affidavit, in order to successfully challenge the probable cause determination. The Defendant does not make this showing. The Defendant's argument assumes that the only possible basis for probable cause would be facts supporting "the conclusion that the site was obviously dedicated to child pornography." First Mot. to Suppress at 11. The Defendant further assumes that this obvious dedication to child pornography must be readily apparent from the homepage, protesting that the images on the homepage were not themselves child pornography. Id. at 11-12.

Far from being an essential component of the probable cause determination, the description of images on the homepage is insignificant compared to the other information found in the

affidavit. Replacing "the user sees images of prepubescent females partially clothed and whose legs are spread" with something like "the user sees an image of a female who appears to be pre-pubescent and is clothed in a short dress and thigh-high fishnet stockings" does not have any appreciable effect on the perceived or actual nature of the website. The Defendant's statement that the description of the logo on the homepage "was a pivotal component of the affiant's allegations in support of probable cause," First Mot. to Suppress at 20, offends common sense: the addition of thigh-high fishnet stockings to a picture of a scantily clad young girl hardly makes an image less sexually suggestive, regardless of whether she can technically be considered "fully clothed." See Matish at *12 (stating that "the logo change lacks significance"); Darby at *7 (noting that the distinction between the images "does not subtract from the sexualized nature" of the later image). As the Defendant points out, the female in the later image merely "appears to be young," and it is unclear that she is prepubescent. First Mot. to Suppress at 9. However, the government need not establish the ages of the subjects to a clear certainty for purposes of probable cause.

The Defendant maintains that, because Playpen's illegal nature was not readily apparent, some computer users may have unwittingly accessed Playpen and then "balked and clicked away."

Reply to Resp. to First Mot. to Suppress at 4. The Defendant argues that, because the NIT Warrant did not distinguish between "accidental browsers" and "people actively seeking child pornography," any "accidental browsers" would have been inappropriately targeted by the NIT Warrant. First Mot. to Suppress at 16-17. The possible means of accessing Playpen are disputed between the government and the defense. The government asserts that, because of Playpen's "hidden service" status on the Tor network, "users must know the exact web address" in order to reach the site. Resp. to First Mot. to Suppress at 6. The Defendant theorizes that Playpen might have been located via an index of sites located on the Tor network. First Mot. to Suppress at 21-22. However, the site need not be "hidden" for the probable cause finding to remain valid. A probable cause finding "does not deal with hard certainties, but with probabilities." Illinois v. Gates, 462 U.S. 213, 231 (1983) (quoting United States v. Cortez, 449 U.S. 411, 418 (1981)). There was a substantial basis for the Magistrate Judge to conclude that a computer user accessing Playpen was doing so in order to view child pornography, whether Playpen was located via an index or by entering the exact web address. See Darby at *8. "[T]he Fourth Amendment requires no more." Gates, 462 U.S. at 236.

The government also claims that certain technical language on the homepage, which dealt with anonymity and with concerns and rules of site privacy, was indicative of the illegal nature of the site. Resp. to First Mot. to Suppress at 9-10. The Defendant disagrees, noting that lawful websites might have similar technical language. First Mot. to Suppress at 22, 28. Playpen's technical language included restrictions on re-posting of materials from other websites and instructions to include previews and encrypted files. NIT Search Warrant and Application at 17-19. The site also warned against using a real email address or disclosing identifying information, and it notified users that Playpen was unable to see users' IP addresses. Id. at 18-19.

Regardless of whether the technical language on the homepage and the site's location on the Tor network indicated criminality, it stands to reason that the casual accidental visitor probably would not locate the Playpen site on the Tor network, let alone create a username and password in order to log into the site, without having any idea as to what the site contained. The fact is that Playpen did contain child pornography, and the affiant knew it contained child pornography. Playpen's content, not its homepage, was the necessary factor in the probable cause determination. See Matish at *11; Darby at *8. There is at least a reasonable probability

that evidence of a crime related to child pornography will be found on a computer that one uses to register with a website that displays child pornography, regardless of whether the homepage alone makes it obvious that the site is a child pornography site. See Darby at *8. Therefore, while the information and image found on the homepage buttressed the conclusion that Playpen was a child pornography site, they were not essential to that conclusion.[3]

The Defendant notes that visitors would have been able to navigate to legal content, such as fictional stories of the "child erotica" variety, without ever accessing child pornography. First Mot. to Suppress at 10, 17. This assertion is contrary to the Defendant's argument that the homepage did not give any indication as to the site's contents. It is improbable that anyone would go to the trouble of registering for the site in order to look for fictional stories likely available elsewhere on the Internet. The user had to (1) either know the URL or locate Playpen via a Tor index, (2) go to the homepage, (3) click past the warning that only members were permitted, (4) create a username, and (5) create a password. NIT Search Warrant and Application at 17-19. Given the totality of the circumstances, substantial support underlies the probable cause finding, and the Defendant has not shown otherwise.

[3] See supra pp. 9-12.

The Defendant next argues in his First Motion to Suppress that "the FBI intentionally or recklessly misled the issuing court about how the site appeared, among other false and misleading statements." First Mot. to Suppress at 2. The affidavit makes clear that the affiant examined Playpen on February 18, 2015, one day before the logo change. See NIT Search Warrant and Application at 17-18, n.3; Resp. to First Mot. to Suppress at 15. Thus, it is unclear that the affiant's description of Playpen as it appeared on that day was a misrepresentation at all, let alone an intentional or reckless one.[4] As discussed above, the appearance of the site's homepage was not necessary to the probable cause finding.

The Defendant then argues that the Warrant was not supported by probable cause, because the Warrant was anticipatory and the triggering event never occurred. First Mot. to Suppress at 3. The Defendant's argument is based on his assertion that the triggering event was logging into the Playpen homepage as it was described by the affiant. Since the

[4] The court held an evidentiary hearing on November 1, 2016. ECF No. 39. Any further hearing into the matter is not warranted, because, as discussed herein, the Defendant has not shown the affiant included a false statement recklessly or intentionally, as is required under Franks v. Delaware, 438 U.S. 154, 171 (1978). Moreover, the allegedly false statement cited by the Defendant was not necessary to the finding of probable cause. See Darby at *9. Accordingly, to the extent the Defendant requests an additional evidentiary hearing, the court **DENIES** the Defendant's request for a Franks hearing.

appearance of the homepage changed, the Defendant's theory goes, the triggering event could not have occurred. Attachment A to the NIT Warrant Application describes the place to be searched pursuant to the warrant. NIT Search Warrant and Application at 3. The Attachment describes the website by URL, not by images found on its homepage. Id. It provides that the "activating computers" are any users or administrators who log into the site—identified by URL only at this point—by entering a username and password. Id. The Defendant's argument that the triggering event did not occur because one additional description of the site in the affidavit was slightly outdated does not "hold water." It is clear from the Application that the triggering event occurred whenever a person logged into the site described by the given URL. While the affidavit's description of Playpen provides explanation of some of the grounds supporting probable cause, the affidavit itself does not establish the triggering event for the NIT Warrant, nor does it need to.

2. Suppression Would Be Inappropriate Here, Even if the Fourth Amendment Was Violated

It is true that the affiant's description of the images depicted on the Playpen homepage was not the same as the images that appeared on the homepage at the time the NIT Warrant Application was filed. However, this inaccuracy is not indicative of the sort of culpability that would warrant

suppression of the fruits of the NIT Warrant search. This FBI operation was a time-sensitive one: the home search of the then-operator of Playpen was the day before the NIT Warrant application was submitted, and the image on the homepage was changed shortly before the search. A delay in the NIT Warrant would have meant a delay in the detection of users downloading child pornography. See Eure at *7. The time-sensitive nature of the operation lessens the culpability of agents who failed to correct what was, in the entire scheme of things, a small error. As courts in the Eastern District have held, under these facts, suppression would not be justified, even if the Fourth Amendment had been violated. See, e.g., id.; Matish at *25. The court, however, is of the opinion that no Fourth Amendment violation occurred here.

II. SECOND MOTION TO SUPPRESS

A. Legal Standards

Rule 41(b) of the Federal Rules of Criminal Procedure has been explicitly incorporated by the Federal Magistrates Act. 28 U.S.C. § 636(a)(1). Rule 41(b) establishes jurisdictional authority of magistrate judges to issue certain search warrants. Violations of Rule 41 are either constitutional or non-constitutional in nature. United States v. Simons, 206 F.3d 392, 403 (4th Cir. 2000). Non-constitutional violations of Rule 41 only merit suppression if (1) the defendant has been

prejudiced by the violation, or (2) there exists evidence of a deliberate disregard of the Rule. Id.

B. Analysis

The Defendant's Second Motion to Suppress asserts that the fruits of the search should be suppressed for two reasons: (1) the NIT Warrant was void, because the Magistrate Judge lacked jurisdiction to issue it under the Federal Magistrates Act; and, alternatively, (2) the Defendant was prejudiced by the government's allegedly deliberate violation of Rule 41(b). Second Mot. to Suppress at 1-2. Courts in the Eastern District of Virginia have already ruled that the Magistrate Judge had jurisdictional authority to issue this same Warrant in regard to three other defendants. See Matish at *17; Darby at *12; Eure at *4.

The Defendant's argument is that Rule 41(b) did not permit the Magistrate Judge to issue the NIT Warrant, because the Rule only permits magistrate judges to issue warrants for searches outside their districts in limited circumstances. See Second Mot. to Suppress at 1-2. Here, the Magistrate Judge issued the NIT warrant against any computer that logged into Playpen and made contact with the server located in the Eastern District of Virginia, regardless of the computer's location. Importantly, Rule 41(b)(4) permits magistrate judges to issue warrants for tracking devices installed within their own districts. Fed. R.

Crim. P. 41(b)(4). Such tracking devices, provided they are installed within the district, can permissibly operate even after the device leaves the district where it was installed. See id. As held by two recent opinions in this district, what occurred here is analogous to these cases. See Matish at *18; Darby at *12. When users logged into Playpen, located on a server in the Eastern District of Virginia, an application launched the NIT coding, only in response to which the users' computers sent messages to the government server. Darby/Eure Hearing Transcript, ECF No. 21-4, at 11:12-13. The Defendant focuses on the locations of the activating computers, but in order to become an activating computer user, the user had to visit Playpen, which was located in the Eastern District of Virginia. Whether the subsequent "tracking" of the identifying information can be said to have physically occurred in this district is a complicated technological question, but it is also a question that misses the point. Here, users picked up an application from a site located in this district. Accordingly, the court **FINDS** that the Magistrate Judge did not violate Rule 41(b) by issuing the NIT warrant.

Regardless, suppression would not be warranted under these circumstances. The Defendant argues for suppression on both constitutional and non-constitutional theories of Rule 41(b) violation. The Defendant's constitutional theory echoes his

general Rule 41(b) violation argument: the NIT Warrant's issuance violated Rule 41(b), voiding the Warrant, and consequently, dooming its execution to violate the Fourth Amendment. However, violation of the Fourth Amendment does not result in automatic suppression of the fruits of the violating search, as discussed above. The conduct of FBI agents here cannot be accurately described as sufficiently culpable or deliberate to warrant suppression. See Darby at *14. They filed their affidavit in support of the NIT Warrant Application in the district where Playpen was located. For users' computers to receive the coding that ultimately tracked the computers' identifying information, users had to visit Playpen. Seeking the NIT Warrant in the Eastern District of Virginia was a reasonable course of action, and their reliance on the Magistrate Judge's determination that the Magistrate Judge had authority to issue the NIT Warrant was objectively reasonable. See Eure at *9. Thus, even if the claims made by the Defendant in his Second Motion to Suppress were accurate, which the court does not find or hold that they are, suppression would still not be warranted under the facts at hand.

III. MOTION TO COMPEL

A. Legal Standards

The government must permit, upon a defendant's request, the inspection of items within the government's control, if (1) the

item is material to defense preparation, (2) the government intends to use the item in its case-in-chief, or (3) the item belongs to the defendant. Fed. R. Crim. P. 16(a)(1)(E). A showing of materiality requires that "pretrial disclosure of the disputed evidence would have enabled the defendant significantly to alter the quantum of proof in his favor." United States v. Caro, 597 F.3d 608, 621 (4th Cir. 2010)(quoting United States v. Ross, 511 F.2d 757, 763 (5th Cir. 1975), cert. denied, 423 U.S. 836). The defendant bears the burden of showing materiality. Id. (quoting United States v. Lloyd, 992 F.2d 348, 351 (D.C. Cir. 1993)). More narrowly, the Due Process Clause requires that, upon request, the government disclose favorable evidence that is material to guilt or punishment of the accused. Brady v. Maryland, 373 U.S. 83, 87 (1963). A materiality showing under Brady requires a reasonable probability that the result would have been different, if the government had disclosed the evidence sought. Caro, 597 F.3d at 619.

Even if evidence is material, the law enforcement privilege can prevent its disclosure. The Fourth Circuit has not directly addressed the law enforcement privilege. However, the privilege has been addressed, in this specific context, by courts in the Eastern District of Virginia. See, e.g., Matish at *5 (stating that the law enforcement privilege is a qualified privilege,

subject to a balancing test, that covers information pertaining to law enforcement techniques and procedures).

B. Analysis

The Defendant argues that the NIT exploit source code and the unique identifier generator are material to his defense. Mot. to Compel at 2. The government argues that (1) these components are not material to defense preparation, and (2) these components are protected by the law enforcement privilege. See Resp. to Mot. to Compel at 4, 21. The Defendant presents a variety of hypothetical situations in which the exploit code and the unique identifier generator could be material to defense preparation. See Reply to Resp. to Mot. to Compel at 3. However, the Defendant has not shown that pretrial disclosure of the disputed evidence would significantly alter the quantum of proof in his favor.

The Defendant seeks disclosure of the unique identifier generator in order to determine whether the NIT accurately identified him. Id. at 7-8. For example, the Defendant discusses the possibility that the code created duplicate identifiers, which he implies would render the identification unreliable. Id. at 6-8. A declaration from FBI Special Agent Daniel Alfin asserts that there were no duplicates, but the Defendant argues he should be able to verify this information, instead of just

relying on the government's claims. Id. at 6. The Defendant has not offered any evidence that there might be duplicates, nor has he explained how such duplicates, if they existed, would be material to defense preparation. The following process of identifying the Defendant was not dependent on the unique identifier generator: (1) the Defendant logged into Playpen; (2) the NIT code communicated with the Defendant's computer; and (3) the Defendant's computer sent identifying information to a government computer in response to the NIT communication. The unique identifier generator created identifiers to match those identified by the NIT with the usernames of Playpen users. Activity records of the username associated with the Defendant could indicate that duplicate identifiers existed, and the government has already offered to provide these to the Defendant in the form of an offline copy of Playpen. See Resp. to Mot. to Compel at 4. The government has also offered to provide the Defendant with "computer instructions that generated the identifying data and the identifying data." Id. at 9. Despite the availability of this evidence to the Defendant, he has not taken advantage of the opportunity to examine it, nor has he produced any evidence, or asserted any reason, beyond mere speculation, as to how discovery of the unique identifier generator would alter the quantum of proof in his favor.

The Defendant also seeks disclosure of the source code for the exploit that enabled the government to deploy the NIT. Mot. to Compel at 1.[5] The Defendant speculates that the exploit could have carried out functions that were outside the scope of the NIT Warrant. Id. at 2. As stated by the government in its Response to Defendant's Motion to Compel, the exploit source code "would only show how the NIT was deployed to McLamb's computer, not what it did once it began interacting with his computer." Resp. to Mot. to Compel at 10. Even if the exploit source code could show what the NIT did once it began interacting with his computer, this showing does not impact the argument that the NIT operation exceeded the scope of the NIT Warrant. The extent of the information seized from the Defendant's computer is already available to the Defendant, because the information itself has already been disclosed to him. Id. at 16. The government has also offered to make the two-way data stream launched by the exploit source code available for defense review. Id. at 11.

The Defendant expresses concern that the exploit could have compromised the security of his computer, allowing other individuals to put child pornography on the machine. Reply to Resp. to Mot. to Compel at 8. He has not submitted any evidence that these things occurred. Special Agent Alfin has said in his

[5] See supra note 2.

declaration that these things did not occur. ECF No. 21-7 at 3. The Defendant's speculation, without more, is insufficient to show materiality. Moreover, the Defendant knows what was in his computer and the government has offered to let the Defendant examine his computer for signs of hacking. Resp. to Mot. to Compel at 13. Again, the Defendant has not taken advantage of this offer, and has presented no evidence that his computer was hacked.

The Defendant also claims that the exploit source code is material because it would enable him to determine whether government representations of how the NIT operated were accurate. Mot. to Compel at 1. However, the Defendant does not explain how, even if the NIT operated differently than the government explained, the exploit source code would be material to his defense. Essentially, the Defendant requests discovery in order to carry out an impermissible "fishing expedition," claiming that he cannot know what evidence he is looking for until he finds it.

Because the Defendant has not shown the materiality of the discovery sought, the Defendant's Motion to Compel is **DENIED.**[6]

---

[6] This court need not reach the issue of whether the law enforcement privilege applies. However, one court within the Eastern District of Virginia has held that the law enforcement privilege would apply to the discovery sought, because the public interest in nondisclosure outweighs the interest of one particular litigant. See Matish at *8. Having reviewed in camera

IV. CONCLUSION

For the foregoing reasons, the court **FINDS** that the NIT Warrant was valid and supported by probable cause, and that neither the exploit source code nor the unique identifier generator are material to defense preparation. Accordingly, the Defendant's Motions to Suppress, ECF Nos. 14 and 15, and the Defendant's Motion to Compel, ECF No. 16, are **DENIED**. The Clerk is **DIRECTED** to send a copy of this Memorandum Opinion and Order to the Federal Public Defender at Norfolk and the United States Attorney at Norfolk.

IT IS SO ORDERED.

/s/
Rebecca Beach Smith
Chief Judge

REBECCA BEACH SMITH
CHIEF JUDGE

November 28, 2016

the Government's Ex Parte, In Camera Classified Memorandum of Law in Support of Assertion of Law Enforcement Privilege, the court here agrees with the conclusion in Matish.